

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-213553

(43)Date of publication of application : 06.08.1999

(51)Int.Cl.

G11B 20/10

G09C 1/00

H04L 9/32

(21)Application number : 10-015788

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 28.01.1998

(72)Inventor : KAMIBAYASHI TATSU  
AKIYAMA KOICHIRO  
TSUJIMOTO SHUICHI

## (54) CONTRACT MANAGING DEVICE AND REPRODUCING DEVICE

## (57)Abstract:

PROBLEM TO BE SOLVED: To make literary works audio-visual within the period of a contract by controlling the reproducing operation of a reproducing device with a signal transmitted to control the receiving operation of broadcasting waves based on an audio-visual contract.

SOLUTION: When a DVD-ROM is inserted into a DVD reproducing device and a reproduction is instructed, the device retrieves license information whose ID is matched with ciphered content information from a license storage part. When the license information corresponding to the ID of the content information exist, the efficiency of the license information is checked, and when the license information are not effective because the effective period of the information is expired or the like, the DVD reproducing device does not perform the decoding and the reproducing of the content information. On the other hand, when the information are effective, the device performs the decoding and the reproducing of the content information. Thus, a charge (a charge being an amount equivalent to a literary property) with respect to the viewing of the content information of a customer is replaced with the reception contract fee of a satellite broadcast in this manner.

## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office



## 【特許請求の範囲】

【請求項1】 記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第1の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第2の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、視聴契約に基づき放送波の受信動作を制御するために配信される信号にて、前記再生装置の再生動作を制御することを特徴とする契約管理装置。

【請求項2】 記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第1の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第2の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、前記制御情報に含まれる識別情報にて特定される再生装置に対してのみ該制御情報に基づくコンテンツ情報の再生が許可されることを特徴とする契約管理装置。

【請求項3】 前記鍵生成情報は、所定期間毎に更新されることを特徴とする請求項1または2記載の契約管理装置。

【請求項4】 放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第1の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第2の鍵情報を生成するために必要な鍵生成情報とに基づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、前記鍵生成情報に基づき生成された第2の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、この復号手段で復号された制御情報に含まれる第1の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、を具備し、前記再生手段は、視聴契約に基づき放送波の受信動作を制御するために配信される信号にて制御されることを特徴とする契約管理装置。

【請求項5】 放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第1の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第2の鍵情報を生成するために必要な鍵生成情報とに基づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であ

って、前記鍵生成情報に基づき生成された第2の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、この復号手段で復号された制御情報に含まれる第1の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、を具備し、前記再生手段は、前記制御情報に含まれる前記識別情報により前記コンテンツ情報の再生の可否を判断することを特徴とする契約管理装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、例えばDVD等の記録媒体にて暗号化されたコンテンツ情報を顧客に（有料）配布し、例えば衛星放送にてコンテンツ情報の復号鍵情報を含む制御情報を再生装置に配信して、そのコンテンツ情報の視聴契約（例えば、視聴期間）に応じて視聴可能にする情報流通システムに関する。

## 【0002】

【従来の技術】近年、デジタル情報処理技術や広帯域ISDN等の通信技術の発達、DVD等の大容量、高画質、高音質を実現する高度な情報記録媒体の開発が進んでいる。このような情報の伝達手段の多様化、高度化が進むにつれ、デジタル化された著作物等がネットワーク、記録媒体などを介して利用者の手元に大量に頒布され、利用者がそれらを自由に利用できる環境が生まれつつある。このような環境は、著作物の無断複製、無断改変、著作物の意図しない流通などが起こる機会を増大させるものであり、著作物の権利者にとって、自己の利益が不当に害されるのではないかという懸念を抱かせるものである。

【0003】このような著作物の権利者の懸念を拭い払えるよう、迅速かつ手軽にデジタル化された著作物を流通させるとともに、適正にそれらを利用できるようなデジタル情報の利用環境を提供できる著作権の保護を前提としたシステムの開発は今後の重要な課題となる。

【0004】DVDは、CD-ROMに代わる大容量のパソコンメディアであるとともに、映画、音楽、ゲーム、カラオケ等、様々な用途への広がり期待でき、このようなDVDの普及を図るために、DVDのタイトル価格を低く抑えたり、レンタルDVD市場への拡大も予想される。従って、このような観点からも、DVD等の記録媒体に記録されたデジタル化された著作物の所有ではなく利用に対して課金するという考えに基づく、情報に対する著作権の保護を前提とした情報の流通システムが不可欠となる。

【0005】一方、デジタル放送は、通信衛星（CS）に始まって、ケーブルTV、地上放送へとデジタル化が進むにつれ、いっそうのサービスの充実が期待されており、これからの放送サービスの主役をつとめてい

くものと思われる。

【0006】デジタル放送の最大の特徴は、情報圧縮技術の導入により、番組の送信に要する周波数の使用効率の向上が図れ、アナログ放送に比較して放送チャンネル数の大幅な増加が可能となったことである。さらに、高度な誤り訂正技術が適用されるため、高品質で均質なサービスの提供が可能となる。

【0007】放送のデジタル化により、多様な情報形態（映像、音声、文字、データ等）によるマルチメディアサービスの提供が可能となり、そのようなサービスを提供するためのシステムも続々登場してきている。

【0008】このようなシステムで、契約内容に基づいてスクランブルを解く、あるいは復号する有料放送サービスを提供する際、契約期間に即した顧客管理が行えなければいけない。契約期間に即した顧客管理とは、例えば、所定の料金の支払により契約された契約期間内に限って契約チャンネルの番組の視聴を可能とするというものである。

【0009】また、受信装置にてスクランブルあるいは暗号を解くための鍵情報は、不正視聴を防止する上からも正当な視聴者のみに（契約チャンネル、契約期間に即して）しかも確実に提供する必要がある。

【0010】

【発明が解決しようとする課題】そこで、本発明は、デジタル化された著作物を迅速かつ手軽に流通させるとともに、デジタル化された著作物の視聴の契約に基づく著作権の保護を前提としたデジタル情報の利用環境を提供する情報流通システムを提供することを目的とする。

【0011】本発明は、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、DVD等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、DVD等の記録媒体に記録されたデジタル化された著作物（コンテンツ情報）の視聴を契約期間に限りて視聴可能にすることができる契約管理装置を提供することを目的とする。

【0012】また、本発明は、放送配信される制御情報に基づき、DVD等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限りて可能にすることができる再生装置を提供することを目的とする。

【0013】

【課題を解決するための手段】本発明の契約管理装置は、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第1の鍵情報を含む暗号化さ

れた制御情報と、該暗号化された制御情報を復号する第2の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、視聴契約に基づき放送波の受信動作を制御するために配信される信号にて、前記再生装置の再生動作を制御することにより、DVD等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、DVD等の記録媒体に記録されたデジタル化された著作物（コンテンツ情報）の視聴を契約期間に限りて視聴可能にすることができる。

【0014】また、本発明の契約管理装置は、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第1の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第2の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、前記制御情報に含まれる識別情報にて特定される再生装置に対してのみ該制御情報に基づくコンテンツ情報の再生が許可されることにより、DVD等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、DVD等の記録媒体に記録されたデジタル化された著作物（コンテンツ情報）の視聴を契約期間に限りて視聴可能にすることができる。

【0015】本発明の再生装置は、放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第1の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第2の鍵情報を生成するために必要な鍵生成情報とに基づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、前記鍵生成情報に基づき生成された第2の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、この復号手段で復号された制御情報に含まれる第1の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、を具備し、前記再生手段は、視聴契約に基づき放送波の受信動作を制御するために配信される信号にて制御されることにより、放送配信されるライセンス情報に基づき、DVD等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限りて可能にすることができる。

【0016】また、本発明の再生装置は、放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第1の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第2の鍵情報を生成するために必要な鍵生成情報とに基

づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、前記鍵生成情報に基づき生成された第2の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、この復号手段で復号された制御情報に含まれる第1の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、を具備し、前記再生手段は、前記制御情報に含まれる前記識別情報により前記コンテンツ情報の再生の可否を判断することにより、放送配信されるライセンス情報に基づき、DVD等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限って可能にすることができる。

#### 【0017】

【発明の実施の形態】以下、本発明の実施形態について図面を参照して説明する。

##### (1) 情報流通サービスの概要

図1は、本発明の実施形態に係る情報流通サービスを提供するためのシステム構成例を示したものである。デジタル化された著作物（例えば映画等）としてのコンテンツ情報は暗号化されて例えばDVD-ROM等の記録媒体（以下、DVD-ROMの場合を例にとり説明する）5に記録されて、例えばレンタル事業会社を介して配布される。

【0018】レンタル事業会社の本部は、系列各店舗に例えば1タイトル毎の暗号化されたコンテンツ情報の記録されたDVD-ROMを配布する。顧客は所望のタイトルのコンテンツ情報の記録されたDVD-ROMを購入しただけでは該コンテンツ情報を視聴することはできない。DVD-ROMに記録された暗号化されたコンテンツ情報を復号、再生するための鍵情報（以下、コンテンツキー）が必要である。このコンテンツキーは、暗号化されて、例えばレンタル会社の本部と提携している衛星放送局200から衛星放送にて各顧客が有する受信装置100に配信される。

【0019】顧客は系列店舗にて該コンテンツ情報のDVD-ROMを購入した際に、少なくとも視聴期間を定めた視聴契約に応じた料金を支払う。この視聴契約に基づき顧客が有するDVD-ROMの再生装置10にて当該DVD-ROMに記録されたコンテンツ情報を顧客が視聴できるようにすることが本発明の目的とするところである。

【0020】なお、DVD-ROMに記録された暗号化されたコンテンツ情報を復号するコンテンツキーは、具体的には（以下の説明では）、衛星放送にて配信される一部暗号化されたライセンス情報（後述）に含まれている。

【0021】ライセンス情報は、本実施形態の場合、例えば、レンタル会社の本部に設置されている契約管理装置にて生成される。顧客が有する再生装置10には、受信装置100（既存のものであることが望ましい）にて

受信された衛星放送にて配信されるライセンス情報が入力し、例えば、別途衛星放送にて配信されるマスターキーシードに基づき生成されたマスターキーにて該ライセンス情報の暗号化部分を復号し、所定の判定処理（詳細は後述する）を実行して、当該顧客の行った視聴契約の有効範囲内での該コンテンツ情報の視聴が可能であると判断したときは、当該ライセンス情報に含まれるコンテンツキーを用いてDVD-ROMに記録された暗号化されたコンテンツ情報を復号し、再生するようになっている。逆に、再生装置10に有効なライセンス情報を入力しなければDVD-ROMに記録された暗号化されたコンテンツ情報を復号することはできない。

【0022】衛星放送にて配信されたライセンス情報は、各放送受信装置100にて受信される。すなわち、本発明の情報流通サービスを利用しようとする顧客は、例えば、従来からある衛星放送の受信サービスを受ける場合と同様、予め当該衛星放送の受信契約を結んでいなければならない。さもなくば、放送受信装置100にてライセンス情報を正しく取得することができない。

【0023】放送受信装置100にて受信されたライセンス情報は、再生装置10へ送られるようになっている。再生装置10は、入力されたライセンス情報を、再生装置機内部のライセンス情報蓄積部に保存する。

【0024】ライセンス情報は、適当なスケジュールに従って、繰り返して放送されている場合がある。このスケジュール方式については後述する。ライセンス情報には、当該ライセンス情報の有効期限情報を含んでいてもよい。

【0025】次に、本発明に係る情報流通サービスの概要を説明する。本発明に係る情報流通サービスを利用しようとする顧客は、このサービスに適応するDVD再生装置10を購入し、さらに、該情報流通サービスを提供している事業会社の系列店舗から所望のタイトルのコンテンツ情報の記録されたDVD-ROMを取得するものとする。

【0026】DVD-ROMには、例えば、図2に示すように、暗号化されたコンテンツ情報が記録されている。所望のタイトルのコンテンツ情報の記録されたDVD-ROMを購入しても、該コンテンツ情報が暗号化されているため、そのままでは視聴することはできない。従って、このコンテンツ情報の記録されたDVD-ROMを購入する際には、必ずしも著作権相当量の料金を支払う必要が無い。すなわち、本発明に係る情報流通サービスを利用しようとする顧客は、例えば、「DVD-ROMそのものの価格+手数料」程度のきわめて低価格でDVD-ROMを取得することが可能となる。

【0027】顧客は、購入した当該DVD-ROMをDVD再生装置10に挿入し、再生を指示すると、DVD再生装置10のライセンス情報蓄積部から、当該コンテンツ情報にIDに一致するライセンス情報を検索する。

初期のライセンス情報が存在しなければ、当該DVD-ROMからコンテンツ情報の再生は行われない。当該コンテンツIDに対応するライセンス情報が存在する場合、DVD再生装置10は、ライセンス情報の有効性をチェックする。有効期限が経過しているなど、ライセンス情報が有効でない場合、DVD再生装置10は当該コンテンツ情報の復号再生を行わない。一方、ライセンス情報が有効であれば、DVD再生装置10は、当該コンテンツ情報の復号、再生を行う。

【0028】このように、顧客のコンテンツ情報の視聴に対する課金（すなわち、著作権相当量の料金）は、衛星放送の受信契約料によって置き換えられる。情報流通サービスを利用しようとする顧客は、まず、放送受信契約を結び、例えば、月々一定金額の受信料を支払う。次に、受信契約者はレンタル事業会社の系列店舗で、好みのタイトルのコンテンツ情報を選ぶ。既に述べたように、暗号化コンテンツが記録された記録媒体の取得には、「記録媒体そのものの価格＋手数料」程度の金額を支払えばよい。その後、顧客は持ち帰ったコンテンツ情報をDVD再生装置10で受信契約に応じて自由に再生することができる。放送受信装置100からDVD再生装置10に、最新の有効なライセンス情報が供給されているからである。

【0029】例えば、ライセンス情報の放送配信によって、7月7日23時59分迄に配信されるライセンス情報（例えばコンテンツID「#21243」のコンテンツ情報に対応するもの）は7月14日23時59分と言う有効期限を持つとする。コンテンツID「#21243」のコンテンツ情報に対応するライセンス情報で、7月21日23時59分と言う有効期限を有するものは、7月8日0時00分以降7月14日23時59分迄に放送され、DVD再生装置10に格納される。これにより、顧客はコンテンツID「#21243」のコンテンツ情報を何時でも再生することができる。

【0030】さて、当該放送の受信契約者が7月22日付けで受信契約を解除する場合、契約解除の旨を7月14日までにレンタル事業会社に通知する。然らば、当該顧客の受信装置100は7月14日23時59分を以ってライセンス放送の受信を中止する。この場合、7月15日0時00分以降に放送される、有効期限7月28日23時59分を有するID「#21243」のライセンス情報は当該受信装置100に配信されず、当該顧客のDVD再生装置10に蓄積されることはない。

【0031】従って、当該顧客は7月21日23時59分以降は、ID「#21243」のコンテンツ情報を視聴できなくなる。以下、より具体的に本発明に係る情報流通サービスを提供するシステムについて説明する。

【0032】DVD-ROMには、図2に示すように、コンテンツキーにて暗号化されたコンテンツ情報と、該コンテンツ情報の識別情報（コンテンツID）と、該コ

ンテンツ情報の内容を紹介するプロモーション用の情報とが記録されている。コンテンツIDとプロモーション用の情報とは暗号化されていない。なお、コンテンツキーは、各コンテンツ情報毎に異なる。また、コンテンツIDは、例えば、タイトル毎に1つずつ付与されているものとする。さらに、コンテンツキーはタイトル毎に予め定められたものである。

【0033】図3は、ライセンス情報のデータ形式を具体例を示したもので、(a)図は、ライセンス情報に受信契約のなされた顧客の有する再生装置のそれぞれを識別するための識別情報（端末ID）を含まない場合のライセンス情報であり、(b)図は当該ライセンス情報を受けとる再生装置を限定するための端末IDを含む場合のライセンス情報を示している。

【0034】図3(a)に示すライセンス情報は、コンテンツ情報の各タイトル毎に1つずつ生成されるもので、少なくとも当該タイトルのコンテンツID、コンテンツキーが含まれている。コンテンツIDは暗号化されず、それ以外の情報（少なくともコンテンツキー）はマスターキーにて暗号化されている。

【0035】図3(a)に示したようなライセンス情報を用いる場合、顧客毎の視聴期間の管理は、例えば、従来からの衛星放送の受信契約管理の場合と同様、各放送受信装置100に対し放送波受信可否を制御するための信号（ON/OFF信号）を送ることにより行ってもよい。すなわち、例えば、顧客の視聴期間の開始時に当該顧客の放送受信装置100に対しON信号を放送配信し、視聴期間の終了時に当該顧客の放送受信装置100に対しOFF信号を放送配信する。放送受信装置100が当該放送受信装置に対して配信されたON信号を受信することで放送波の受信を開始し、OFF信号を受信することで放送波の受信を不可とする制御を行うようになっていく。

【0036】図3(b)に示すライセンス情報は、少なくとも当該タイトルのコンテンツID、コンテンツキーと、当該ライセンス情報を受けとる再生装置を特定する端末IDが含まれている。コンテンツIDは暗号化されず、それ以外の情報（少なくともコンテンツキー、端末ID）はマスターキーにて暗号化されている。

【0037】なお、図3(b)に示すライセンス情報は、端末IDとして、単に個々の再生装置の端末IDを1つのみ記載して、各顧客毎に当該ライセンス情報を生成、配信してもよいし、例えば端末IDの下数桁を端末IDとして記載して、1度に複数の再生装置が受け取れるようにしてもよい。後者の方がライセンス情報の配信効率がよいことは言うまでもない。

【0038】図3(b)に示すライセンス情報を用いる場合、顧客毎の視聴期間の管理は、例えば、ライセンス情報の端末IDに契約期間がきれた顧客の再生装置10の端末IDを記載しないことで行うことができる。この

場合、再生装置10のそれぞれがライセンス情報に含まれる端末IDと自身の端末IDとを比較してライセンス情報を取り込むか否かをチェックすることになる。契約期間中は自身の端末IDそのものが記載された、あるいは自身の端末IDを含むライセンス情報が頻繁に配信されるが、契約期間がきた時点からライセンス情報には自身の端末IDは記載されなくなる。従って、再生装置10は、有効なライセンス情報を得られないがためにDVD-ROMに記録された暗号化されたコンテンツ情報の復号、再生が行えないことになる。

【0039】ライセンス情報の暗号化には、次の様な特徴を持った暗号化方式を利用することが望ましい。

1) コンテンツID、コンテンツキーなどのデータを適当な順序で並べる。ここで、各データをフィールドと呼ぶことがある。

【0040】2) 適当なアルゴリズムに従って、1)のビット列の順序を攪乱する。この際、広い範囲でビット攪乱が行われることが望ましい。

3) 2)のデータを適当な鍵と暗号方式で暗号化する。1)をそのまま暗号化しないのは、次の理由による。すなわち、通常の暗号方式は、あらかじめ定められた適当なビット長毎に暗号化を行うことを繰り返す。従って、2)の攪乱を行うことにより、ライセンス情報の各フィールドが分離・改変される危険性を低下させることが可能である。

#### 【0041】(2) 契約管理装置

図4は、本実施形態に係る契約管理装置の構成例を示したもので、図1の地上局200に設置されて用いられる。

【0042】地上局200は、図3(a)あるいは図3(b)に示したようなライセンス情報とマスターキーシードを放送配信する。ライセンス情報中、コンテンツID以外の部分はマスターキーにて暗号化されている。ライセンス情報の機密性の向上のためにマスターキーは一定期間毎に更新することが好ましい。そのために、再生装置10にてマスターキーを生成するために必要な情報、すなわち、マスターキーシードを(定期的あるいはマスターキー更新時に)放送配信するようになっている。

【0043】さて、図4の契約管理装置は、ライセンス情報の生成、暗号化を行って放送配信するためのものである。顧客との間で放送受信契約がなされると、その契約内容(コンテンツID、視聴期間等)が、契約ユーザデータベース(DB)1に登録される。

【0044】契約ユーザDB1には、図5に示す形式でデータが蓄えられる。図5において受端末IDは顧客の有する再生装置10の端末IDであり、この端末IDに対応させて視聴契約のなされたコンテンツIDと視聴期間とが予め定められた形式で記憶されている。

【0045】シードデータベース(DB)3は、マスタ

ーキー生成用のマスターキーシードから生成されるマスターキーをそのシードID及び有効期限とともに、図6に示す形式で格納している。シードDB3にはシードIDに対応するマスターキーシードも格納されている。

【0046】コンテンツキーデータベース(DB)4は、タイトル毎のコンテンツキーをコンテンツIDに対応させて図7に示す形式で格納している。次に、図3

(b)に示したようなライセンス情報を生成し、これを放送装置13を使って受信装置に送る手順を図8に示すフローチャートを参照して説明する。

【0047】ライセンス情報生成制御部9は、ライセンス情報生成部8に対し、ライセンス情報生成の指示を送る(ステップS11)。この指示とは、例えば「1997年12月1日から1ヶ月間契約している契約ユーザのライセンス情報を送れ」なる内容のもので、予め定められた形式のビット列で表現されたものでもよい。このような指示が出されるとライセンス情報生成部8では契約ユーザDB1から1997年12月1日から少なくとも1ヶ月間契約しているユーザ情報(図5参照)を検索して、当該情報を読み込む(ステップS12～ステップS13)。

【0048】ここで、契約期間の最小単位は1ヶ月で、契約有効期限は1日にはじまり月末に終了するとし、マスターキーもこの契約最小期間に固有なものとする。すなわち、11月のマスターキーは12月のそれとは異なるものを用い、それぞれの月内では変更しないものとする。

【0049】次に、付加情報生成部8は、コンテンツキーDB4からコンテンツID毎のコンテンツキーを検索し(ステップS15)、また、シードDB3から1997年12月1日から1997年12月31日に有効なシードに対応したマスターキーを検索する(ステップS16)。

【0050】以上によって得られた情報(コンテンツID、該コンテンツIDに対応するコンテンツキー、各ユーザの契約内容)をもとに、付加情報生成部8では、図3(b)に示すようなライセンス情報を生成し、コンテンツID以外の情報を暗号化する(ステップS17)。ここで生成されたライセンス情報は順次付加情報生成制御部9、放送装置13に送られる。

【0051】放送装置13は、ライセンス情報を所定の周波数帯域の放送波に変換して受信装置に向けて放送配信する(ステップS18)。スケジューリング部14は、ライセンス情報DB5に格納されたライセンス情報を配信する際、あるいは、マスターキーシードを配信する際、各ユーザ側の受信装置にて確実にライセンス情報、マスターキーシードが受信されるように配信制御を行うものである。

【0052】すなわち、例えば、受信契約後、契約変更



時、契約解約時、および、人気のタイトルのコンテンツIDに対するライセンス情報を送信する際には、当該ライセンス情報を頻繁に送る必要があり、そのためのライセンス情報の配信スケジューリングに従って、ライセンス情報の配信制御を行うのが、スケジューリング部14である。

【0053】ライセンス情報生成部8にて生成されたライセンス情報には、配信日時を示すタイムスタンプが含まれていてもよい。タイムスタンプの示す日時は時計15にて計時されたできる限り正確なものであり、また、再生装置10からは各種判定処理に用いる基準となる時刻となり得るものである。なお、タイムスタンプはもちろん暗号化されていない。

【0054】図3(a)に示すようなライセンス情報を用いる場合には、契約ユーザDB1を検索する必要がない。すなわち、図8のステップS11でライセンス情報生成の指示を受けたライセンス情報生成部8は、ステップS15に進み、コンテンツキーDB4からコンテンツID毎のコンテンツキーを検索し、また、シードDB3から1997年12月1日から1997年12月31日に有効なシードに対応したマスターキーを検索し(ステップS16)、図3(a)に示すようなライセンス情報を生成し、コンテンツID以外の情報を暗号化する(ステップS17)。

【0055】なお、マスターキーシードは、ライセンス情報の暗号化に用いられたマスターキーに対応するものをライセンス情報の配信と同時にあるいは適宜配信されている。

#### 【0056】(3) 再生装置

図9は、本実施形態に係る再生装置10の構成例を示したもので、図10は、再生装置10のライセンス判定ユニット208の構成例を示したものである。

【0057】以下、図11、図12に示すフローチャートを参照して再生装置10およびライセンス判定ユニット208の各構成部およびこれらの動作について説明する。放送受信装置100は、地上局200からの放送波を受信し、放送配信されたライセンス情報とマスターキーシードが再生装置10のフィルタ202に入力する(ステップS21)。

【0058】フィルタ202ではライセンス情報とマスターキーシードとを分別し、マスターキーシードであれば、それをライセンス判定ユニット208へ転送し、ライセンス情報であれば、それをライセンス情報蓄積部204へ転送する(ステップS22～ステップS25)。

【0059】ライセンス判定ユニット208では、マスターキー生成部801にてマスターキーシードからマスターキーを生成して、マスターキー格納部802に格納する(ステップS26)。マスターキーを生成する際には、予め契約管理装置との間で定められた同一のアルゴリズムを用いてマスターキーシードから共有鍵としての

マスターキーを生成するようにしてもよい。また、ライセンス判定ユニット208のマスターキー生成部801では、新たにマスターキーシードが入力される度にそれを用いてマスターキーを生成して、それをマスターキー格納部802に格納されている前回までのマスターキーに上書きして保持することにより、マスターキーが更新されてもその都度その更新された新たなマスターキーを得ることができる。

【0060】ライセンス情報蓄積部204では、入力されたライセンス情報をコンテンツID別に保存する。すなわち、ライセンス情報が入力される度に、それに含まれるコンテンツIDをチェックし、既に同じコンテンツIDのライセンス情報が保存されている場合は、それに上書きしていく。ライセンス情報にタイムスタンプが含まれている場合は、それに示される日時をチェックして、所定期間経過したものは廃棄する、新たに入力されたライセンス情報で上書きしていく、等の制御が行える。

【0061】さて、再生装置10にDVDディスクが挿入されると(ステップS31)、DVDドライブ206は、まず、当該ディスクからコンテンツIDを読み出し、ライセンス情報選択部207へ転送する(ステップS32)。ライセンス情報選択部207は、当該コンテンツIDを有するライセンス情報を、ライセンス情報蓄積部204から検索する(ステップS33)。当該コンテンツIDを有するライセンス情報が存在するときは、それをライセンス判定ユニット208に転送する(ステップS34～ステップS35)。当該ライセンスIDを有するライセンス情報が見つからないとき、あるいは、あったとしてもタイムスタンプに示される時刻から無効なもの(期限切れ)と判断できるときは、その後の処理を中止する。

【0062】ライセンス判定ユニット208の復号部804では、マスターキー格納部802に格納されているマスターキーを用いてライセンス情報選択部207から転送されたライセンス情報を復号する(ステップS36)。

【0063】ここで、図3(b)に示したようなライセンス情報の場合のライセンス判定ユニット208の判定部805における判定処理について説明する。この場合、判定部805では、復号されたライセンス情報に含まれていた端末IDにID格納部803に予め格納されている自身の端末IDが一致するか、あるいは含まれているかをチェックする。自身の端末IDと一致あるいは自身の端末IDが含まれていれば当該ライセンス情報は有効と判定し、復号されたライセンス情報に含まれていたコンテンツキーをデコーダ(例えば、MPEG2デコーダ)209へ転送する(ステップS37～ステップS38)。それ以外の場合は、当該ライセンス情報は無効と判定し、以後の処理は中止する。

【0064】次に、図3(a)に示したようなライセンス情報の場合のライセンス判定ユニット208の判定部805における判定処理について説明する。この場合、判定部805では、特に判定処理はおこなわなくてもよく、そのまま、復号されたライセンス情報に含まれていたコンテンツキーをMPEG2デコーダ209へ転送する(ステップS37～ステップS38)。この場合の顧客毎の視聴期間の管理は、例えば、従来からの衛星放送の受信契約管理の場合と同様、各放送受信装置100に対し放送波受信可否を制御するための信号(ON/OFF信号)を送ることにより行っているため、放送受信装置100が一旦OFF信号を受けたときはそれ以後ON信号を再び受信するまで放送波の受信動作を行うことはないからである。

【0065】DVDドライブ206では、DVDディスクから暗号化されたコンテンツ情報を読み取って、それをMPEG2デコーダ209へ転送する(ステップS39)。

【0066】MPEG2デコーダ209はライセンス判定ユニット208から転送されてきたコンテンツ情報を用いて該暗号化されたコンテンツ情報を復号し、さらにD/A変換して所定の表示装置へ出力する(ステップS40からステップS41)。

【0067】なお、ライセンス情報にタイムスタンプが含まれている場合、ライセンス判定ユニット208に時計が具備されているとき、判定部805では、タイムスタンプにて示されている日時と、この時計にて計時されている日時とを比較して、当該ライセンス情報の有効/無効を判定してもよい。また、ライセンス情報に含まれるタイムスタンプに示され時刻情報を用いて、当該時計の時間設定を行うようにしてもよい。これらの詳細処理動作は、特願平9-122511号に記載されている。

【0068】

【発明の効果】以上説明したように、本発明の契約管理装置によれば、DVD等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、DVD等の記録媒体に記録されたデジタル化された著作物(コンテンツ情報)の視聴を契約期間に限って視聴可能にすることができる。

【0069】また、本発明の再生装置によれば、放送配信されるライセンス情報に基づき、DVD等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限って可能にすることができる。

【図面の簡単な説明】

【図1】本発明の実施形態に係る情報流通サービスを提供するためのシステム構成例を示した図。

【図2】コンテンツ情報の記録された例えばDVD-ROM等の記録媒体の記録データの構成例を示した図。

【図3】ライセンス情報のデータ構成例を示した図。

【図4】契約管理装置の構成例を示した図。

【図5】契約ユーザDBに記憶されるユーザ情報のデータ構成例を示した図。

【図6】シードDBに記憶される情報のデータ構成例を示した図。

【図7】コンテンツキーDBに記憶される情報のデータ構成例を示した図。

【図8】図4の契約管理装置の動作を説明するためのフローチャート。

【図9】再生装置の構成例を示した図。

【図10】図9のライセンス判定ユニットの構成例を示した図。

【図11】図9の再生装置および図10のライセンス判定ユニットの動作を説明するためのフローチャート。

【図12】図9の再生装置および図10のライセンス判定ユニットの動作を説明するためのフローチャート。

【符号の説明】

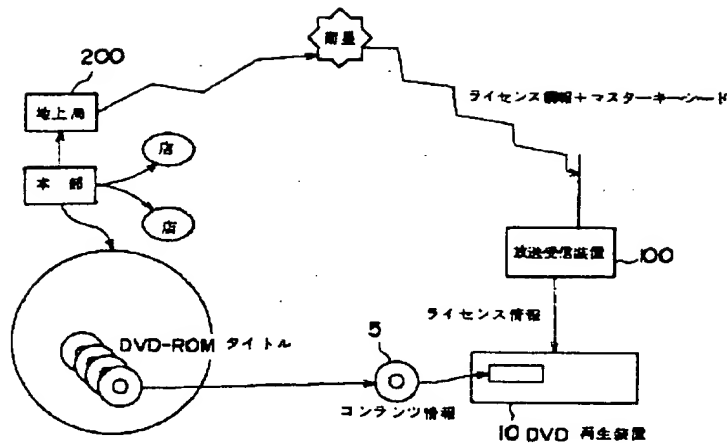
放送管理装置

- 1…契約ユーザデータベース
- 3…シードデータベース
- 4…コンテンツキーデータベース
- 5…ライセンス情報データベース
- 8…ライセンス情報生成部
- 9…ライセンス情報生成制御部
- 12…ライセンス情報出力要請部
- 13…放送装置
- 14…スケジューリング部

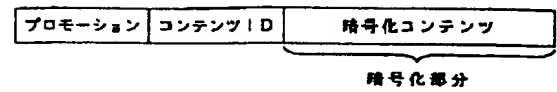
再生装置

- 202…フィルタ
- 204…ライセンス情報蓄積部
- 206…DVDドライブ
- 207…ライセンス情報選択部
- 208…ライセンス判定ユニット
- 209…MPEGデコーダ
- 801…マスターキー生成部
- 802…マスターキー格納部
- 803…ID格納部
- 804…復号部
- 805…判定部

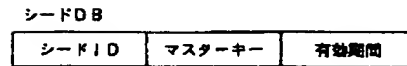
【図1】



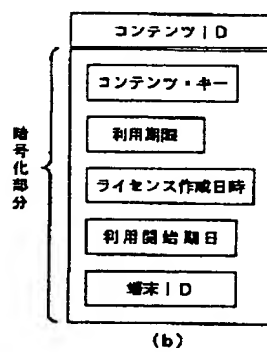
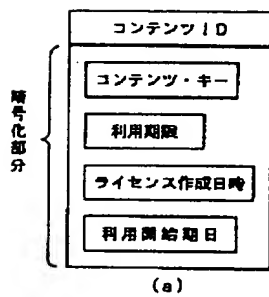
【図2】



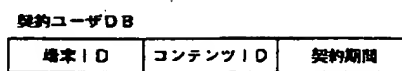
【図6】



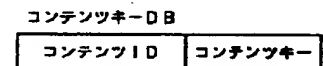
【図3】



【図5】

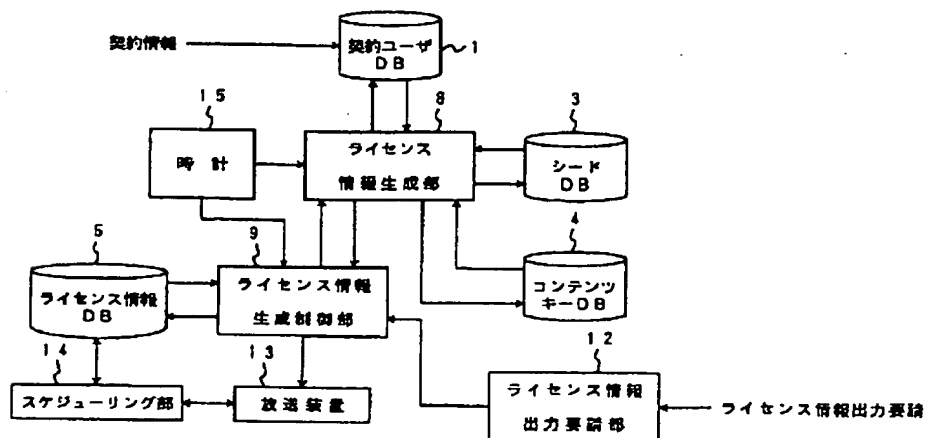


【図7】

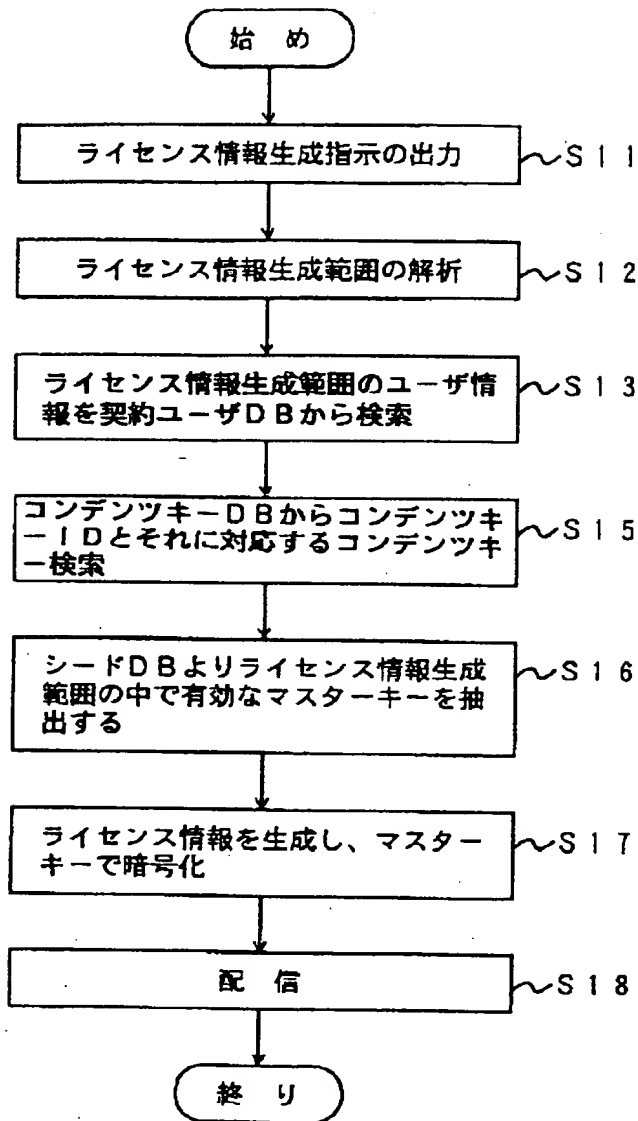


【図4】

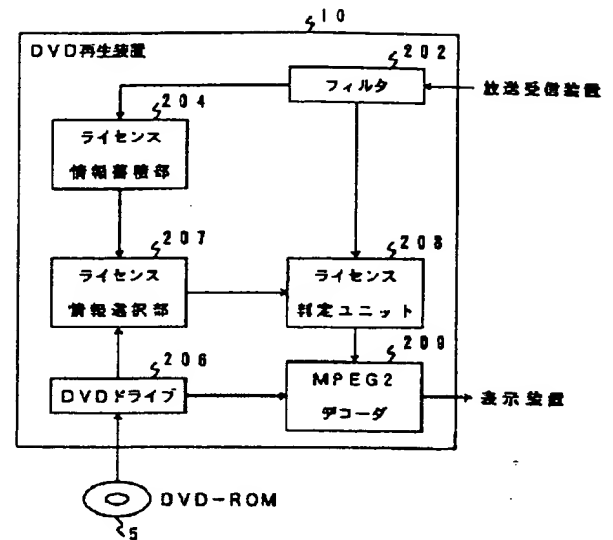
## 契約管理装置



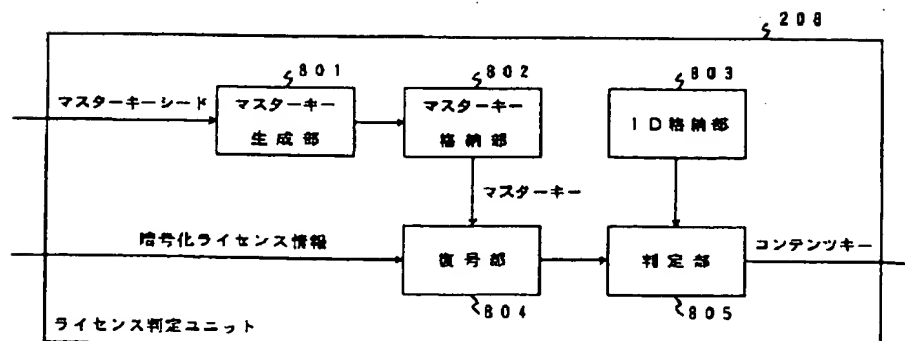
【図8】



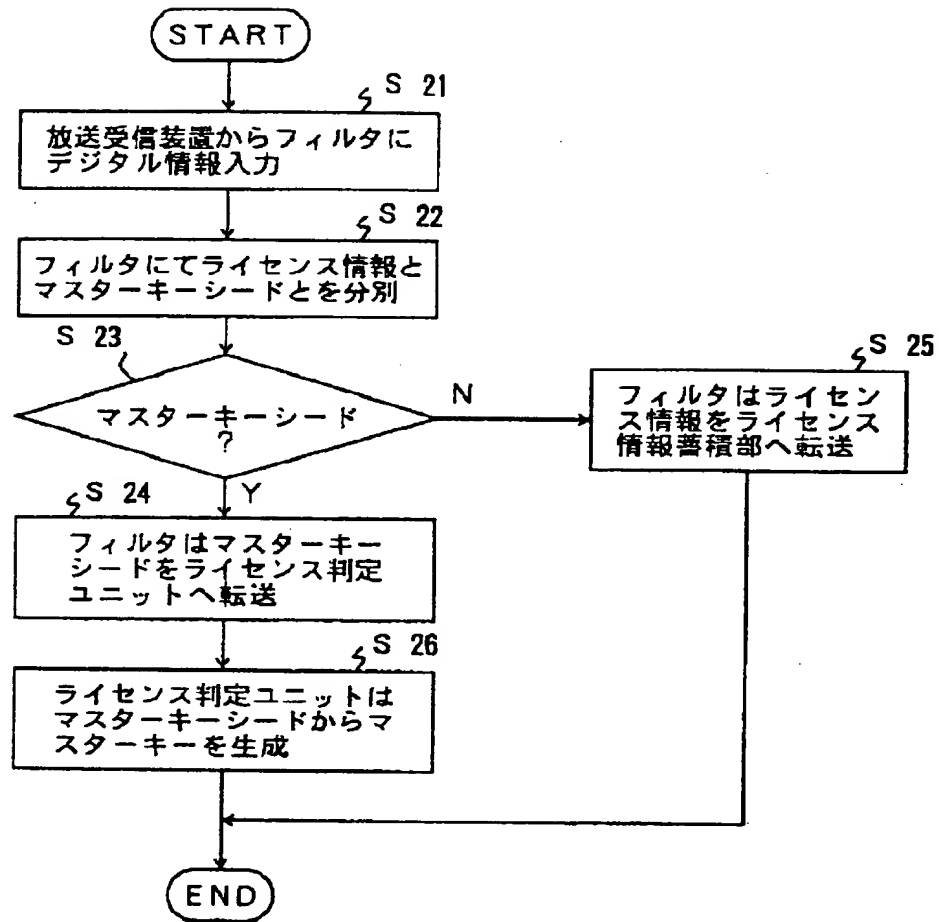
【図9】



【図10】



【図11】



【図12】

